www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16719-16723

Spoofing Attack Detection And Localization In Wireless Networks

V Jagadheeswar Reddy, M.Nirmala
M.Tech,CSE
Aurora's Technological & Research Institute
Hyderabad,Telangana,India
E-Mail:jagadhiswar.v@gmail.com
Assistant Professor
Aurora's Technological & Research Institute
Hyderabad,Telangana,India
E-Mail:madhavapeddynirmala@gmail.com

Abstract: Abstract: Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. In this paper, we propose to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for (1) detecting spoofing attacks; (2) determining the number of attackers when multiple adversaries masquerading as a same node identity; and (3) localizing multiple adversaries. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. We then formulate the problem of determining the number of attackers as a multi-class detection problem. Cluster-based mechanisms are developed to determine the number of attackers. When the training data is available, we explore using Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, we developed an integrated detection and localization system that can localize the positions of multiple attackers. We evaluated our techniques through two test beds using both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in two real office buildings. Our experimental results show that our proposed methods can achieve over 90% Hit Rate and Precision when determining the number of attackers. Our localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

Keywords: Wireless network security, spoofing attack, attack detection, localization.

I. INTRODUCTION

In a large-scale network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks such as network resource utilization attack and denial-of-service attack quickly.

Therefore, it is important to

- Detect the presence of spoofing attacks,
- Determine the number of attackers, and
- Localize multiple adversaries and eliminate them.

Most existing approaches to address potential spoofing attacks employ cryptographic schemes [1], However; the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead. Further, cryptographic methods are susceptible to node compromise, which is a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned. In this work, we propose to use RSS-based spatial correlation, a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Since we are concerned with attackers who have different locations than legitimate wireless nodes, utilizing spatial information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries. An added advantage of employing spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices [5] themselves.

We focus on static nodes in this work, which are common for spoofing scenarios. We addressed spoofing detection in mobile environments in our other work . The works that are closely related to us are Proposed the use of matching rules of signal prints for spoofing detection, modeled the RSS readings using a Gaussian mixture model and used RSS and K-means cluster analysis to detect spoofing attacks. However, none of these approaches have the ability to determine the number of attackers when multiple adversaries use a same identity to launch attacks, which is the basis to further localize multiple adversaries after attack detection. Although studied how to localize adversaries, it can only handle the case of a single spoofing attacker and cannot localize the attacker if the adversary uses different transmission power level.

II.PROBLEM DEFINITION

Detecting multiple spoofing attackers using wireless network.Determine the number of attackers, and localize multiple adversaries and eliminate them[3].

III OUR APPROACH

Algorithms:

RADAR GRIDDED ALGORITHM:

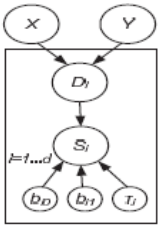
. The RADAR-Gridded algorithm is a scene-matching localization algorithm extended from. RADAR-Gridded uses an interpolated signal map, which is built from a set of averaged RSS readings with known (x, y) locations. Given an observed RSS reading with an unknown location, RADAR[15] returns the x, y of the nearest neighbor in the signal map to the one to localize, where "nearest" is defined as the Euclidean distance of RSS points in an N-dimensional signal space, where N is the number of landmarks.

Area Based Probability (ABP): ABP also utilizes an interpolated signal map. Further, the experimental area is divided into a regular grid of equal sized tiles. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution with mean as the expected value of RSS reading vector **s**. ABP then computes the probability of the wireless device being at each tile Li, with i = 1...L, on the floor using Bayes' rule:

$$P(L_i|\mathbf{s}) = \frac{P(\mathbf{s}|L_i) \times P(L_i)}{P(\mathbf{s})} \qquad (30)$$

Given that the wireless node must be at exactly one tile satisfying $\sum^{L}_{i=1}P(Li|\mathbf{s}) = 1$, ABP normalizes the probability and returns the most likely tiles/grids up to its confidence α.

Bayesian Networks (BN): BN localization is a multilateration algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization. Below figure shows the basic Bayesian Network used for our study. The vertices X and Y represent location; the vertex si is the RSS reading from the landmark; and the vertex Di represents the Euclidean distance between the location specified by X and Y and the ith landmark. The value of si follows a signal propagation model $si = b_{0i}+b_{1i}$ logDi, where b_{0i}, b_{1i} are the parameters specific to the ith landmark.



Bayesian graphical model in our study

The distance $Di = \sqrt{(X - x_i)^2 + (Y - y_i)^2}$ in turn depends on the location (X, Y) of the measured signal and the coordinates (x_i, y_i) of the ith landmark. The network models noise and outliers by modeling the s_i as a Gaussian distribution around the above propagation model, with variance τi: $si \sim N(b_{0i} + b_{1i}$ logDi, $\tau_i)$. Through Markov Chain Monte Carlo (MCMC) simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

IV .IMPLEMENTATION DETAILS

Communication Module:

- This module is responsible for take number of nodes from user and display the nodes in tree diagram
- After that, application will calculate Distance and Euclidean for each node and display in a table format.

Distance = sqrt ((x1-x2)2+(y1-y2)2)

Where,

x1 = x position of node 1
x2 = x position of node 2
y1 = y position of node 1
y2 = y position of node 2

- Then we select a file to transfer over network from one node to another node and then we show receiving status to end user.
- After transferring file application will find RSS (received signal strength) value for each node.

del(si)=10gamma log(d2/d1)+del(x)
where,
d1=Euclidean Distance of Node 1
d2=Euclidean Distance of Node 2

Cluster Analysis Module:

- This module is responsible for dividing all nodes in network into 2 clusters.
- Then application will find RSS [7] Received Signal Strength) value and Euclidean value all nodes in each cluster.
- After dividing nodes into clusters, application will find medoid in each cluster and then calculate the distance between those 2 medoid nodes.

Distance between Medoids(DM) =mod(mi-mj)
Where,
mi = Medoid of Cluster_1
m j= Medoid of Cluster_2

- AfteR calculate distance between medoids(DM),then we check for attack detection

If Distance between Medoids > Threshold
Then presence of spoofing attack.

.

Energy Dynamics Module:

- This module is responsible for calculate parathion energy(EP) and merging energy(EM).
- The application will calculate parathion energy(EP) by using following formula

Ep(k)=((1/(na+nb))*(sum1+sum2))
Where,
na = number of Nodes In Cluste_1
nb = number of Nodes In Cluste_2
sum1 = sum of Euclidean Distance Of Nodes In Cluster 1
sum2 = sum of Euclidean Distance Of Nodes In Cluster 2

The application will calculate merging energy(EM) by using following formula

Em(k)=((1/(na+nb))*(sum1+sum2))
Where ,
na = number of Nodes In Cluste_1
nb = number of Nodes In Cluste_2
sum1 = sum of rss value Of Nodes In Cluster 1
sum2 = sum of rss value Of Nodes In Cluster 2

Detection & Localization of Attackers Module

- This module is responsible for Detection & Localization of Attackers [4][16].
- The Detection of number of attackers can be determined by

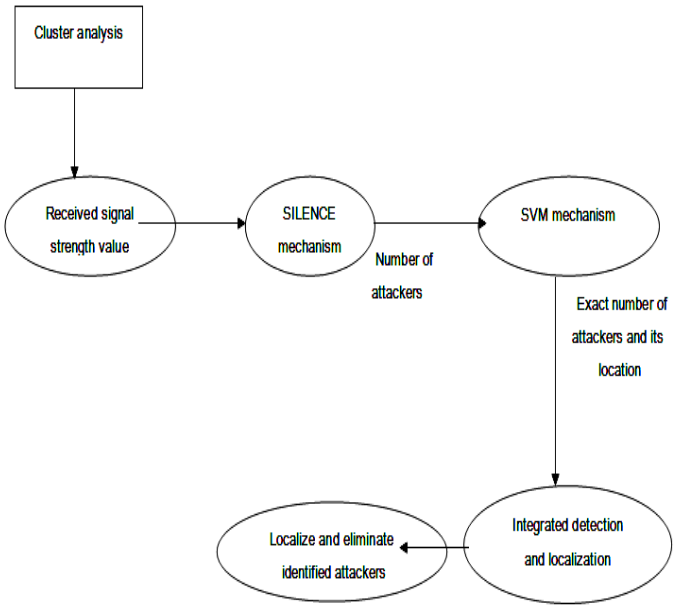
When K = n with Ep(n) > Em(n)
Where,
n = number of clusters
Ep(n) = Partition Energy
Em(n) = Merging Energy

- Integration Detection and Location is find by

Si=b0i+bli log Di
Where,
b0i = x position of node i
bli = y position of node i
Di = Euclidean Distance between the Nodes

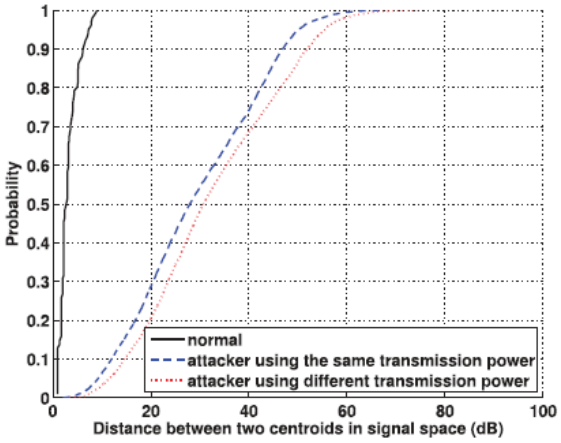
- Then application will find which nodes are attacked and how many attackers then localize the attackers.
- Application will generate graph of the time complexity of the location of nodes.

Data Flow Diagram:



V. EXPERIMENTAL RESULTS

Figures show the Cumulative Distribution Function of Dm in signal space under both normal conditions as well as with spoofing attacks. We observed that the curve of Dm shifted greatly to the right under spoofing attacks. Thus, when Dm > t, we can declare the presence of a spoofing attack.



VI .CONCLUSION AND FUTURE WORK

In this paper, Our approach can detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. We developed SILENCE, a mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than other methods under study, such as Silhouette Plot and System Evolution that use cluster analysis alone. Additionally, when the training data is available, we explored using Support Vector Machines (SVM) based mechanism to further improve the accuracy of determining the number of attackers present in the system. To validate our approach, we conducted experiments on two test beds through both an 802.11 [6]network (Wi-Fi) and an 802.15.4 (ZigBee) network in two real office building environments. We found that our detection mechanisms are highly effective in both detecting the presence of attacks with detection rates over 98% and determining the number of adversaries, achieving over 90% hit rates and precision simultaneously when using SILENCE and SVM-based mechanism. Further, based on the number of attackers determined by our mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of our approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.

VII REFERENCES

1. J. Bellardo and S. Savage, “802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,” in *Proceedings of the USENIX Security Symposium*, 2003, pp. 15 – 28.
2. F. Ferreri, M. Bernaschi, and L. Valcamonici“Access points vulnerabilities to dos attacks in 802.11 networks,” in *Proceedings of the IEEE Wireless Communications and Networking Conference*, 2004.
3. D. Faria and D. Cheriton, “Detecting identity-based attacks in wireless networks using signalprints,” in *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, September 2006.
4. Q. Li and W. Trappe, “Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks,” in *Proc. IEEE SECON*, 2006.
5. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks,” in *Proc. IEEE IPDPS*, 2005.

6. A. Wool, “Lightweight key management for ieee 802.11 wireless lans with key refresh and host revocation,” *ACM/Springer Wireless Networks*, vol. 11, no. 6, pp. 677–686, 2005.
7. Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, “Detecting 802.11 MAC layer spoofing using received signal strength,” in *Proc. IEEE INFOCOM*, April 2008.
8. J. Yang, Y. Chen, and W. Trappe, “Detecting spoofing attacks in mobile wireless environments,” in *Proc. IEEE SECON*, 2009.
9. Y. Chen, W. Trappe, and R. P. Martin, “Detecting and localizing wirelss spoofing attacks,” in *Proc. IEEE SECON*, May 2007.
10. M. bohge and W. Trappe, “An authentication framework for hierarchical ad hoc sensor networks,” in *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, 2003, pp. 79–87.
11. L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, “Fingerprints in the ether: using the physical layer for wireless authentication,” in *Proceedings of the IEEE International Conference on Communications (ICC)*, June 2007, pp. 4646–4651.
12. V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless device identification with radiometric signatures,” in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 116–127.
13. F. Guo and T. Chiueh, “Sequence number-based mac address spoof detection,” in *Recent Advances in Intrusion Detection*, 2006, pp. 309–329.
14. L. Sang and A. Arora, “Spatial signatures for lightweight security in wireless sensor networks,” in *The 27th Conference on Computer Communications, INFOCOM 2008.*, 2008, pp. 2137–2145
15. P. Bahl and V. N. Padmanabhan, “RADAR: An in-building RF-based user location and tracking system,” in *Proc. IEEE INFOCOM*, 2000.
16. E. Elnahrawy, X. Li, and R. P. Martin, “The limits of localization using signal strength: A comparative study,” in *Proc. IEEE SECON*, Oct. 2004.

1.